AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph beginning on page 5, line 4 with the following amended paragraph:

Smartcards provide some of the above mentioned functionality, but smartcards do not present an ideal solution. First, personal keys are only valuable to the user if they offer a single, widely accepted secure repository for digital certificates and passwords. Smartcard readers are relatively expensive, and are not in wide use, at least in the United States, and are therefore unsuited to the task.

Please replace the paragraph beginning on page 13, line 7 with the following amended paragraph:

The ~~personal key~~ host computer has an interface including a USB driver module 266 communicatively coupled to an application program interface (API) 260 having a plurality of API library routines. The API 260 provides an interface with the application 110 to issue commands and accept results from the personal key 200. In one embodiment, a browser 262, such as the browser available from NETSCAPE, Inc. operates with the API 260 and the public key cryptographic standard (PKCS) module 264 to implement a token-based user authentication system.

Please replace the paragraph beginning on page 13, line 20 with the following amended paragraph:

Ultimately, the personal key 200 identifies the possessor to the outside world through the host computer 102, but there is no guarantee that the person in possession of the personal key 200 is the actual owner, because the personal key may have been lost or stolen. Security can be increased with the use of personal passwords and the like, but this solution is not ideal. First, the use of a single password raises the very real possibility that the password may have been compromised (after all, the thief may know the user, and hence, the user's password). Also, requiring the entry of a password multiple times increases the chance that malicious software executing in the host computer 102 or the remote computer 134 may eavesdrop on the password or personal identification. The use of multiple passwords is no solution because one of the reasons for using the personal key 200 is to relieve the user of the need to remember a number of passwords. Another problem with passwords is that hacking methods can be employed to circumvent the password protection or to discover the password itself. This is especially problematic in context of a personal key 200 which in most cases, depends on data entered in a host computer ~~120~~ 102 peripheral such as the keyboard 114 and transmitted via the input/output port 130, rendering the personal key 200 vulnerable to hacking.

Please replace the paragraph beginning on page 30, line 12 with the following amended paragraph:

While the foregoing has been described with a single light emitting device ~~646,~~ 616, the present invention can also advantageously embody two or more light emitting devices, or devices emitting energy in other wavelengths. For example, the foregoing can be implemented with a three color LED (red, yellow and green), or three one-color LEDs to transfer personal key 200 information to the user.

Please replace the paragraph beginning on page 30, line 17 with the following amended paragraph:

In addition to or as an alternative to the foregoing, information regarding the operation of the personal key 200 is provided by an aural transducer such as a miniaturized loudspeaker or piezoelectric transducer. Such aural information would be particularly beneficial to users with limited or no vision. For example, the aural transducer can be used to indicate that the personal key 200 has been inserted properly into the host computer ~~120~~ 102 I/O port 130.

Please replace the paragraph beginning on page 33, line 3 with the following amended paragraph:

The foregoing pressure sensitive devices may also be used to provide a binary input to the personal key 200. For example, the user's PIN or password can be entered by applying pressure to the first pressure sensitive device 702 and the second pressure sensitive device 704 in the proper order in rapid succession. In this way, a user password or PIN defined as "10100010111" may be entered by depressing the first pressure sensitive device ~~502~~ 702 to indicate a "0" and the second pressure sensitive device 704 to indicate a "l."

Please replace the paragraph beginning on page 34, line 11 with the following amended paragraph:

To ameliorate this problem, one embodiment of the present invention utilizes a "squeeze to sign" authorization technique, in which some direct user action is required to authorize the use of identified secret values stored in the personal key 200. For instance, if a private key (such as the secret 406) or PIN stored in the memory 214 of the personal key 200 is identified as requiring a "squeeze to sign" authorization, firmware executing in the processor 212 of the personal key 200 requires direct user input via the input device ~~410~~ 218 or the data transceiver 252 before honoring any request from the host computer 102 or the remote computer/server 134 that involves the use of the private key or personal information. Ordinarily, the private key and/or other personal information is designated as requiring direct authorization by an associated value or flag in the memory 214. Such data may also be designated as "use-only" indicting that the data cannot be read directly from the key under any circumstances. The data may be shared with no other entity (as would often be the case with a PIN), or may be a value shared with the trusted entity and used for authorization, such as the secret 406. For example, private keys can be used as the secret 406 to perform authorization via hash functions. In such cases, the secret value 406 is typically a shared secret such as a DES key or a password. Since secret values 406 can be stored in the memory 214 of the personal key 200, before distributing the personal key 200 to the user, the secret value 406 need not be made available in plaintext form at any time.

Please replace the paragraph beginning on page 38, line 33 with the following amended paragraph:

FIG. 10 is a flow chart illustrating an embodiment of the present invention in which the PIN is entered directly into the personal key 200. In block 1002, a command is issued which requires access to the user's PIN, such as VerifyPIN and ModifyPIN commands listed in Table 6. At block 1004, ~~The~~ the personal key 200 accepts ~~1004~~ the command, and if necessary, prompts the user for the PIN, as shown in block 1006. This may be accomplished with the display 122, one of the output devices 222, or any combination thereof. Preferably, this is accomplished via a communication path distinct and inaccessible from the USB interface 204. Using one of the input device 218 embodiments described above, at block 1010 the user provides the PIN to the personal key 200. Using a value stored in the memory 214, at block 1012 the processor 212 in the personal key 200 validates the user-entered PIN. In one embodiment, this is accomplished by comparing the user-provided value directly with a value stored in the memory 214. At block 1014, the ~~The~~ personal key then provides ~~1014~~ a response indicating the validity of the PIN, which is accepted by the API 260 at block 1016. The response indicates whether the user supplied PIN was valid.

Please replace the paragraph beginning on page 39, line 12 with the following amended paragraph:

The processor is also optionally communicatively coupled to one or more light emitting devices ~~216~~ 616 or other visual display device to provide a visual indication of the activities or status of the personal key 200. The processor 212 may also be communicatively coupled with an aural device to provide a vibrational or audio data to the user of the status or activities of the personal key 200.